EXHIBIT 3

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 04-60001-CR-COOKE/Brown (s)(s)(s)(s)(s)

UNITED STATES OF AMERICA

vs.

ADHAM AMIN HASSOUN,
a/k/a "Abu Sayyaf,"

Defendant.
_____/

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANT HASSOUN'S MOTION FOR PRODUCTION AND DISCLOSURE OF FISA MATERIALS AND SUPPRESSION OF FISA EVIDENCE (U)

269
TK

TABLE OF CONTENTS

I. BACKGROUND (U) 2

II. SUMMARY OF THE FACTS (U) 4

[CLASSIFIED INFORMATION REDACTED]

III. OVERVIEW OF FISA (U) 4

A. THE APPLICATION (U) 4

B. THE CERTIFICATION (U) 6

C. THE FISC'S ORDER (U) 6

D. USE OF FISA INFORMATION IN CRIMINAL PROSECUTIONS (U) 8

E. THE DISTRICT COURT'S REVIEW IN CRIMINAL PROSECUTIONS (U) 8

IV. ARGUMENT (U) 9

A. THE COURT SHOULD DENY THE DEFENDANT'S MOTION FOR THE PRODUCTION AND DISCLOSURE OF FISA MATERIALS AND REVIEW THE FISA MATERIALS *IN CAMERA* AND *EX PARTE* (U) 9

B. THE LAW APPLICABLE TO FISA COLLECTION (U) 17

(1) Statutory Requirements (U) 17

(2) Standard of Review (U) 20

(3) The First Amendment (U) 22

(4) This Court Should Not Suppress The FISA Evidence Even If This Court Disagrees With The FISC's Findings Of Probable Cause (U) 23

(5) FISA's Certification Requirements As To The Purpose Of The Surveillances Were Satisfied (U) 26

(a) Standard of Review of Certification Requirement (U) 27

(b) Neither Concurrent Criminal and Foreign Intelligence Investigations Nor Information-Sharing Between Intelligence and Law Enforcement Agents Negates the Government's Certification of Purpose (U) 30

(6) FISA's Requirement That The Information Could Not Reasonably Be Obtained By Normal Investigative Techniques Was Satisfied (U) 32

(7) Hassoun Has Failed To Establish the Requisite Preliminary Showing Necessary to Obtain a Hearing Pursuant to Franks v. Delaware, 438 U.S. 154 (1978) (U) 33

(8) Minimization Under FISA (U) 36

C. THE FISA COLLECTION AT ISSUE (U) 44

(1) [CLASSIFIED INFORMATION REDACTED] 44

(a) [CLASSIFIED INFORMATION REDACTED] 44

(b) [CLASSIFIED INFORMATION REDACTED] 44

(2) [CLASSIFIED INFORMATION REDACTED] 44

(a) [CLASSIFIED INFORMATION REDACTED] 44

(b) [CLASSIFIED INFORMATION REDACTED] 44

(c) [CLASSIFIED INFORMATION REDACTED] 44

(3) [CLASSIFIED INFORMATION REDACTED] 44

(a) [CLASSIFIED INFORMATION REDACTED] 44

(b) [CLASSIFIED INFORMATION REDACTED] 45

(c) [CLASSIFIED INFORMATION REDACTED] 45

(d) [CLASSIFIED INFORMATION REDACTED] 45

(e) [CLASSIFIED INFORMATION REDACTED] 45

(f) [CLASSIFIED INFORMATION REDACTED] 45

(f) [CLASSIFIED INFORMATION REDACTED] 45

(g) [CLASSIFIED INFORMATION REDACTED] 45

(h) [CLASSIFIED INFORMATION REDACTED] 45

(i) [CLASSIFIED INFORMATION REDACTED] 45

(4) [CLASSIFIED INFORMATION REDACTED] 45

(a) [CLASSIFIED INFORMATION REDACTED] 45

(b) [CLASSIFIED INFORMATION REDACTED] 45

(c) [CLASSIFIED INFORMATION REDACTED] 45

(d) [CLASSIFIED INFORMATION REDACTED] 45

(e) [CLASSIFIED INFORMATION REDACTED] 45

(f) [CLASSIFIED INFORMATION REDACTED] 45

(g) [CLASSIFIED INFORMATION REDACTED] 45

(h) [CLASSIFIED INFORMATION REDACTED] 45

(5) [CLASSIFIED INFORMATION REDACTED] 45

(a) [CLASSIFIED INFORMATION REDACTED] 45

(b) [CLASSIFIED INFORMATION REDACTED] 45

(c) [CLASSIFIED INFORMATION REDACTED] 45

(6) [CLASSIFIED INFORMATION REDACTED] 45

V. CONCLUSION (U) 46

CERTIFICATE OF SERVICE 47

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 04-60001-CR-COOKE/Brown (s)(s)(s)(s)(s)

UNITED STATES OF AMERICA

vs.

ADHAM AMIN HASSOUN,
a/k/a "Abu Sayyaf,"

Defendant.
_____/

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANT HASSOUN'S MOTION FOR PRODUCTION AND DISCLOSURE OF FISA MATERIALS AND SUPPRESSION OF FISA EVIDENCE (U)

The United States of America, through its undersigned Attorneys respectfully submits this memorandum of law in opposition to defendant Adham Amin Hassoun's (Hassoun) motions for production of FISA applications, orders and related materials (hereinafter collectively referred to as "FISA materials") and suppression of FISA-obtained and derived evidence.[1] The government respectfully submits that after this Court conducts an *in camera* and *ex parte* review of the

[1] On March 13, 2006, defendant Kifah Jayyousi (Jayyousi) filed a Motion to Adopt Defendant Hassoun's motions, including Hassoun's motion for production and disclosure of FISA materials and motion to suppress FISA evidence, after his motion filing deadline had passed. This Court denied his Motion to Adopt Hassoun's motion to suppress FISA materials. However, this Court granted his Motion to Adopt Hassoun's motion for production of FISA materials. Each argument made by the government in opposition to defendant Hassoun's motion for the production and disclosure of FISA materials also applies to Jayyousi. Therefore, the government hereby asserts all of its arguments stated in the Memorandum on that issue in opposition to Jayyousi's adopted motion for production and disclosure of FISA materials, and respectfully requests that this Court, after its *in camera* and *ex parte* review, deny both defendants' requests for the production and disclosure of FISA materials for the reasons set forth in this Memorandum. (U)

documents relevant to these motions, as required by the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, it will conclude that the FISA collection at issue was lawfully authorized and conducted, and that none of the classified documents sought by the defendants should be disclosed. Accordingly, defendants' motions should be denied. (U)

I. BACKGROUND (U)

On November 17, 2005, defendants Hassoun, Jayyousi, and Jose Padilla (Padilla) were charged in a fifth superseding indictment with conspiring to murder, maim, or kidnap persons in a foreign country, in violation of 18 U.S.C. § 956; and conspiring to provide and providing material support to terrorists, in violation of 18 U.S.C. §§ 2339A(a) and 371, and 18 U.S.C. § 2339A. (U)

On April 27, 2004, the government notified defendant Hassoun, following the third superseding indictment, that it intended to offer into evidence, or otherwise use or disclose at pre-trial hearings, trial, and at other proceedings in this case, information obtained and derived from collection authorized pursuant to FISA. Defendants Jayyousi and Padilla were also notified that the government intended to offer or otherwise use such information against them in this case. (U)

On February 13, 2006, defendant Hassoun moved for the production of all FISA materials and for disclosure of all other electronic surveillance. In his motion, the defendant seeks information from the National Security Agency (NSA), the United States Army, the United States Air Force, the DOD Counterintelligence Field Activity, the Army Intelligence and Security Command, the Army Counterintelligence Center and the Air Force Office of Special Investigations. Defendant Hassoun also filed a separate motion to suppress the FISA evidence.

(U)

On February 16, 2006, the District Court referred defendant Hassoun's motions, including both of his FISA related motions (D.E.#200, D.E. #201), to United States Magistrate Judge Stephen T. Brown pursuant to 28 U.S.C. § 636. In his motion for disclosure, defendant Hassoun argues that the Court should order the production of FISA materials apparently even before the Court conducts an *in camera, ex parte* review as mandated by the provisions of FISA. The defendant further seeks suppression of evidence obtained or derived from any FISC-authorized electronic surveillance which he may have been a third party. (Hassoun Mot. To Suppress at 14-16.) (U)

In support of its opposition to the defendant's motions, the government is submitting a classified memorandum to be provided to the Court Security Officer, as well as this unclassified version to be served on the defense. The unclassified version is nearly identical to the classified version with the exception of the references to the classified information contained in the FISA materials.[2] In addition, the United States is separately filing with this Court the following documents: an unclassified Declaration and Claim of Privilege of the Attorney General of the United States; a classified Declaration of a high-ranking official of the FBI, in support of the Attorney General's Declaration and Claim of Privilege; classified Declarations by the FBI regarding the applicable minimization procedures; and certified copies of the classified FISA materials.[3] The unclassified documents will be served on defense counsel and filed with the

---

[2] As the result of deletion of the classified information from the unclassified version, the pagination and Table of Contents are different in the two versions of the memorandum. (U)

[3] A classified index of the FISA materials also is being provided to the Court. (U)

Clerk of Court; the classified documents will be submitted to the Court for *in camera*, *ex parte* review as part of a Sealed Exhibit as required by FISA. (U)

These papers are submitted not only to oppose the defendant's motions relating to the FISA evidence, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera* and *ex parte* review of the classified documents listed above; (2) find that the FISA collection at issue was lawfully authorized and conducted; and (3) order that none of the classified documents, nor any of the classified information contained therein, be disclosed, and instead, that they be maintained by the United States under seal.[4] (U)

II. SUMMARY OF THE FACTS (U)

[CLASSIFIED INFORMATION REDACTED]

III. OVERVIEW OF FISA (U)

Prior to addressing the defendant's arguments for disclosure of FISA materials and suppression of the FISA-obtained and derived evidence, a brief overview of FISA's requirements is provided below. (U)

A. THE APPLICATION (U)

FISA establishes a statutory procedure whereby the Executive Branch may collect foreign intelligence information "without violating the rights of citizens of the United States." United

---

[4] As of this date, defendant Padilla has not yet filed motions seeking disclosure of FISA related materials or suppression of the FISA evidence. Padilla has until May 1, 2006 to file motions. Nevertheless, pursuant to FISA, the United States requests that the Court determine that the FISC-authorized collection at issue here was lawfully authorized and conducted, and in the event any such motions are made, to deny such motions. See, e.g., 50 U.S.C. § 1806(g) ("If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.") (U)

States v. Hammound, 381 F.3d 316, 332 (4th Cir. 2004); see United States v. Johnson, 952 F.2d 565, 571 (1st Cir. 1992). FISA enumerates the requirements that must be met before electronic surveillance may begin.[5] With a few exceptions not pertinent here, FISA requires that a court order be obtained before any such surveillance may be conducted. Prior to submitting a request to the FISC, FISA also requires a substantial review of an application by the Attorney General and by a high-ranking Executive Branch official with national security or defense responsibilities. See 50 U.S.C. §§ 1804(a) & (a)(7). (U)

An application for electronic surveillance pursuant to FISA must contain, among other things: (1) "the identity, if known, or a description of the target of the electronic surveillance;" (2) a statement of the facts and circumstances supporting the belief that the target "is a foreign power or an agent of a foreign power," and that the facilities or places "at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;" (3) a statement of the proposed minimization procedures to be followed; (4) "a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;" (5) a statement regarding the need for any physical entry to conduct the surveillance; (6) a statement regarding previous FISA applications involving the same persons, facilities or places, and any action taken pursuant to those applications; (7) a statement outlining the required duration of the surveillance; and (8) a statement regarding the need, if any, for more than one surveillance device. See 50 U.S.C. § 1804(a)(1)-(11) (setting forth items required in application for FISA order.) (U)

---

[5] The statutory requirements for an order authorizing a physical search pursuant to FISA are identical in all material respects to the requirements for an order authorizing electronic surveillance pursuant to FISA. See 50 U.S.C. §§ 1821-1829. As a result, the citations set forth herein are to the electronic surveillance provisions of the statute. (U)

B. THE CERTIFICATION (U)

In addition to the above-referenced requirements, FISA mandates that a high-ranking Executive Branch official with national security responsibilities certify the following: (1) that the information sought is "foreign intelligence information," a term that is defined in section 1801(e); (2) that the "purpose" of the surveillance is to obtain foreign intelligence information (for applications filed prior to the passage of the USA PATRIOT Act on October 26, 2001),[6] or that a "significant purpose" is to obtain foreign intelligence information (for applications filed after the effective date of the Act);[7] (3) that the foreign intelligence information sought cannot reasonably be obtained by normal investigative techniques; and (4) that the information being sought fits within a specified category or categories of "foreign intelligence information" as set forth in section 1801(e). See 50 U.S.C. § 1804(a)(7)(A)-(E). Finally, the Attorney General must approve applications for FISA surveillance before they are presented to the FISC. 50 U.S.C. § 1804(a)(7). (U)

C. THE FISC'S ORDER (U)

Following the Attorney General's approval, the application is then submitted to one of the United States District Court Judges appointed by the Chief Justice of the United States to serve on the FISC.[8] Before the FISC may approve the requested surveillance or search, the judge must find that: (1) the President has authorized the Attorney General to approve FISA applications; (2)

---

[6] See Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). (U)

[7] [CLASSIFIED INFORMATION REDACTED]

[8] The appointment of judges to the FISC is provided for in 50 U.S.C. § 1803(a). Prior to the passage of the USA PATRIOT Act, seven judges comprised the FISC. The Act changed the number of judges to eleven. (U)

the application has been made by a "Federal officer" and has been approved by the Attorney General; (3) there is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power, and that the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (4) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h); and (5) the application contains all statements and certifications required by section 1804 and, if the target is a United States person,[9] the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) and any other information furnished under section 1804(d)." 50 U.S.C. § 1805(a)(1)-(5) (setting forth the necessary findings by the FISC.) (U)

If the FISC is satisfied that the FISA application has met the statutory provisions, which will be outlined in greater detail below, and it has made all of the necessary findings, the FISC may issue an *ex parte* order authorizing the surveillance. The order must identify the target of the electronic surveillance; the location or facility at which the surveillance will be directed, the type of information to be sought, the means of conducting the surveillance, the duration of the surveillance, the authorized coverage of the surveillance device(s), and the applicable minimization procedures. See 50 U.S.C. §§ 1805(b)(1)(A)-(F). Under FISA, before the passage of the USA PATRIOT Act, electronic surveillance of agents of a foreign power generally, and initially, lasted 90 days. See 50 U.S.C. § 1805(e)(1). Extensions could have been granted, but only if the United States submitted another application in compliance with FISA. See 50 U.S.C.

---

[9] A "United States person" means, among other things, "a citizen of the United States [or] an alien lawfully admitted for permanent residence." 50 U.S.C. § 1801(i). (U)

§ 1805(e)(2). The FISC also retained the authority to review, prior to the end of the search or surveillance operation, the United States' compliance with the requisite minimization procedures. See 50 U.S.C. § 1805(e)(3). (U)

D. USE OF FISA INFORMATION IN CRIMINAL PROSECUTIONS (U)

FISA authorizes the use of information obtained or derived from any FISC-authorized electronic surveillance in a criminal prosecution, so long as the use comports with FISA's requirements, including the requirement for advance authorization by the Attorney General. See 50 U.S.C. § 1806(b). Evidentiary use of FISA obtained and derived information is permitted in proceedings before federal, state, and local courts, provided that proper notice is given to each "aggrieved person" against whom the information is to be used.[10] See 50 U.S.C. § 1806(c)-(d) (notification provisions.) Upon receiving notice, the aggrieved person may then move to suppress the use of FISA information on the grounds that the information was unlawfully acquired or the surveillance was not made in conformity with an order of authorization or approval. See 50 U.S.C. § 1806(e). (U)

E. THE DISTRICT COURT'S REVIEW IN CRIMINAL PROSECUTIONS (U)

The trial court has jurisdiction to determine the legality of the FISA surveillance at issue. See 50 U.S.C. § 1806(f). The district court, however,

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the

---

[10] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). (U)

aggrieved person was lawfully authorized and conducted.

50 U.S.C. § 1806(f); see United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (holding that the "proper procedure" is *in camera* and *ex parte* review when the Attorney General files an affidavit pursuant to section 1806(b).) Upon the filing of such an affidavit or declaration[11] by the Attorney General, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance ***only where such disclosure is necessary*** to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f) (emphasis added.) If the district court is able to make an accurate determination in regard to the legality of the surveillance based on an *in camera, ex parte* review of the materials submitted by the United States, then the court may not order disclosure of any of the FISA materials. Badia, 827 F.2d at 1464 (affirming district court's refusal to disclose FISA materials where the court was able to determine the legality of the surveillance without disclosure.) (U)

IV. ARGUMENT (U)

A. THE COURT SHOULD DENY THE DEFENDANT'S MOTION FOR THE PRODUCTION AND DISCLOSURE OF FISA MATERIALS AND REVIEW THE FISA MATERIALS *IN CAMERA* AND *EX PARTE* (U)

The Attorney General has filed a declaration pursuant to FISA in this case. As a result, FISA mandates that the Court conduct an *in camera, ex parte* review of the FISA materials at issue to determine whether the collection was lawfully authorized and conducted. E.g., 50 U.S.C. § 1806(f); see Badia, 827 F.2d at 1464. The federal courts have repeatedly held that FISA

---

[11] Whenever an "affidavit" is required, a declaration may be filed with "like force and effect." 28 U.S.C. § 1746. (U)

anticipates that *in camera, ex parte* determination is to be the rule and disclosure and an adversary hearing the "exception occurring only when necessary." United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (emphasis in original.) Thus, this Court may not order disclosure of pertinent FISA materials unless it is unable to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f)-(g). When the Attorney General files a declaration that disclosure or an adversary hearing would harm national security (as he has done in this case), the propriety of the disclosure cannot even be considered unless the district court responsible for reviewing the suppression motion has concluded that it is unable to make an accurate determination of the legality of the surveillance ***after*** reviewing the United States' submissions. Because the documents that have been provided for the Court's *in camera, ex parte* review provide more than sufficient information for the Court to accurately determine the legality of the FISA collection at issue, the government respectfully submits that the FISA materials may not be disclosed. (U)

FISA's Congressionally-mandated procedures govern the circumstances under which the disclosure of FISA materials may take place. In fact, "Congress was adamant, in enacting FISA, that [it's] 'carefully drawn procedure[s]' are not to be 'bypassed by the inventive litigant using a new statute, rule, or judicial construction.'" Belfield, 692 F.2d at 146 (quoting H.R. Rep. No. 95-1283, 95th Cong., 2d Sess. at 91 (hereafter "House Report"), and citing S. Rep. No. 95-701, 95th Cong., 2d Sess. at 63 (hereafter "Senate Intelligence Report") reprinted in 1978 U.S.C.C.A.N 3904.) Congress was fully cognizant of the competing national security interest of the Executive Branch in maintaining the secrecy of the surveillance procedures used in foreign intelligence investigations on the one hand, and the interests of "aggrieved persons" in litigating claims of

infringement upon Fourth Amendment privacy rights on the other. As the Belfield court of appeals explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to 'reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights.' In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance.

Belfield, 692 F.2d at 148 (footnotes omitted) (citing Senate Intelligence Report at 16 (1978); see also ACLU Foundation of So. Cal. v. Barr, 952 F.2d 457, 465 (D.C. Cir. 1992) (construing Belfield as precedent for the proposition that section 1806(f) "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance"); Ott, 827 F.2d 473, 477 (9th Cir. 1987) (noting "that Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question.") Thus, if disclosure of the FISA materials is not necessary to resolve the legality of the FISA surveillance in this case within the meaning of the statute, then disclosure may not be ordered. (U)

Every single federal district court and court of appeals in this district and elsewhere that has examined this issue has concluded that disclosure of FISA materials to the defense was not necessary to its inquiry into the legality of the surveillance. Rather, all of the courts addressing motions to suppress FISA evidence have been able to reach a conclusion as to the legality of the

surveillance based on an *in camera* and *ex parte* review. See Badia, 827 F.2d at 1463-4; United States v. Damrah, 412 F.3d 618, 624 (6th Cir. 2005) (district court did not abuse its discretion in denying defendant's motion to compel disclosure of FISA materials absent a showing of misrepresentation of the facts or any other presentation warranting disclosure); In re Grand Jury Proceedings of the Special April 2002 Grand Jury, 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court has ever ordered disclosure of FISA materials); United States v. Squillacote, 221 F.3d 542, 553-554 (4th Cir. 2000); United States v. Johnson, 952 F.2d 565, 571-572 (1st Cir. 1991); United States v. Isa, 923 F.2d 1300, 1306 (8th Cir. 1991); In re Grand Jury Proceedings, 856 F.2d 685, 688 (4th Cir. 1988); United States v. Sarkisasian, 841 F.2d 959, 965 (9th Cir. 1988); United States v. Ott, 827 F.2d at 475; United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984); Belfield, 692 F.2d at 147; United States v. Butenko, 494 F.2d 593, 607 (3d Cir. 1974) (en banc); United States v. Sattar, No. 02 CR. 395 JGK, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003); United States v. Bin Laden, 126 F. Supp. 2d 264, 287 (S.D.N.Y. 2000); United States v. Rahman, 861 F. Supp. 247, 250-251 (S.D.N.Y. 1994) (no disclosure necessary to "make an accurate determination of whether the surveillance at issue was lawfully authorized and conducted"), aff'd, 189 F.3d 88 (2d Cir. 1999); United States v. Spanjol, 720 F. Supp. 55, 59 (E.D. Pa. 1989) (In enacting FISA, Congress intended to restrict, as much as constitutionally possible, discovery of FISA materials); United States v. Nicholson, 955 F. Supp. 588, 592 & n.11 (E.D. Va. 1997) ("[T]his court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance") (collecting cases); United States v. Thomson, 752 F. Supp. 75, 79 (W.D.N.Y. 1990) (same) (collecting cases.) (U)

Furthermore, the complexity of a case is not the proper benchmark for whether disclosure

of FISA materials is warranted. Neither are large numbers of applications and orders, nor the number of pages of briefing that a district court may have to review, determinative of whether such disclosure is necessary. See In re Grand Jury Proceedings, 856 F.2d at 688 ("50 applications"); United States v. Squillacote, 221 F.3d at 553-554 ("more than 20 FISA applications.) Instead, the legal question for the Court is whether the documents submitted are sufficient to allow the court to make a determination of legality. Here, the FISA materials submitted are fully and facially sufficient to allow this Court to make a determination of legality; they "are straightforward and readily understood." See In re Matter of Kevork, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985). (U)

The government has a legitimate interest in protecting national security with respect to FISA materials. In addition to the specific harm that would result from the disclosure of the FISA materials in the instant case, which is outlined in the classified Declaration of a high ranking FBI official in support of the Attorney General's Declaration, the underlying rationale for nondisclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." United States v. Ott, 637 F. Supp. 62, 65 (E.D. Cal. 1986), aff'd, 827 F.2d 473 (9th Cir. 1987). In addition to the protection that is needed with respect to highly sensitive and classified sources, protection is also needed with respect to classified methods and techniques. (U)

Thus, when a question is raised as to whether the disclosure of classified information, sources, methods or techniques would harm the national security, the federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of determining whether foreign agents, spies and terrorists are

capable of piecing together a mosaic of information which, when revealed, could reasonably be expected to harm the national security of the United States. See United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods.") (U)

As a result, FISA materials, unlike criminal wiretap-materials, should be withheld from defense counsel – even defense counsel who may possess a security clearance – unless the Court determines that the disclosure of the materials "is necessary to make an accurate determination as to the legality of the surveillance." 50 U.S.C. § 1806(f). The security clearance that a defense attorney may possess is, therefore, simply irrelevant to the issue of whether he or she has a "need to know" within the meaning of FISA. See United States v. Ott, 827 F.2d at 477; United States v. Bin Laden, 126 F.Supp.2d at 286; see also Executive Order 13292, § 6.1(z) (requiring that a "need to know" determination be made prior to the disclosure of classified information to anyone, including those who possess a security clearance.) If a court concludes that it is capable of accurately determining the legality of the FISA collection at issue, then even a defense attorney with a security clearance does not have a "need to know." Indeed, if a court were to order disclosure of FISA materials in the face of a claim of privilege by the Attorney General simply because a defendant's attorney had a security clearance, without a finding that such disclosure was "necessary" within the meaning of FISA, then this would be contrary to well established precedent, and tantamount to a rewriting of a statute that was passed by the legislative branch and signed into law by the President. (U)

Hassoun also argues that disclosure of the FISA materials is warranted due to the possibility of unspecified misstatements of fact. Hassoun offers no factual basis for his claim other than to rely upon the FISC's decision in In re All Matters Submitted to the FISC, 218 F. Supp. 2d 611 (For. Intel. Surv. Ct. 2002), rev'd, In re Sealed Case, 310 F.3d 717 (For. Intel. Surv. Ct. of Review 2002), in which reference was made to seventy-five FISA applications that contained inaccuracies. Neither the circumstances of this case, nor the content of the FISA materials, compels disclosure. (U)

As a threshold matter, the United States Department of Justice's Office of Intelligence Policy and Review, which has supervisory responsibility over all matters before the FISC, has confirmed that none of the applications at issue in this case are among the seventy-five cited by the FISC. (U)

The defendant's speculative and unsupported accusations of generalized misstatements based on observations in In re All Matters is insufficient to establish that disclosure is "necessary to make an accurate determination of the legality of the surveillance" in this case. 50 U.S.C. § 1806(f). Since the defense has been provided the summaries of pertinent intercepted communications, as well as many transcripts, they are in a position to direct the Court's attention to any specific areas of concern in regard to the manner in which the surveillance was conducted that have been raised from his review of those FISA surveillance materials. The defense, however, has not done so. After this Court conducts its own review of the FISA-related materials, this Court will be quite able to independently make an accurate determination of the legality of the FISC orders without disclosure. (U)

Defendant's claims notwithstanding, there is nothing extraordinary about the FISA

collection ordered in this case that would justify this case becoming the first "exception" to the rule; that is, where the unprecedented production and disclosure of highly sensitive and classified FISA materials is ordered. Again, the practical question for the court is whether the submissions permit the court to make an accurate determination that the collection was lawfully authorized and conducted. The government respectfully submits that there is nothing atypical about what this Court needs to do beyond applying the same procedure all other district and appellate courts have engaged in when confronted with a defendant's motion for disclosure of FISA materials. The government has confidence that this Court will be able to review the FISA applications, orders and related materials, and make the appropriate findings consistent with the applicable law. The FISA materials have been methodically organized and compiled for the Court, and the statute and the case law are clear. Thus, in view of the classified submissions to this Court, the Attorney General's Declaration and Claim of Privilege, which is supported by a Declaration of a high ranking FBI official,[12] and in light of the applicable law, the government respectfully submits, there is no basis upon which to order disclosure of the FISA materials. (U)

Accordingly, the Court should deny defendant Hassoun's motion and should not order the production and disclosure of any of the FISA materials.[13] (U)

---

[12] A separate basis for the non-disclosure of classified FISA materials, in addition to the statutory mechanism set forth in FISA, is the invocation by the United States of its classified information and national security privilege, a privilege which is well established. See C & S Air Lines v. Waterman SS Corp., 333 U.S. 103, 111 (1948) ("[The President] has available intelligence services whose reports are not and ought not to be published to the world: and are "properly" held "secret"); United States v. Nixon, 418 U.S. 683, 710 (1974) (distinguishing a national security privilege from an executive privilege); United States v. Yunis, 867 F.2d at 623-24 (comparison of government's "classified information privilege" to the "informant privilege.") (U)

[13] A district court order requiring the disclosure of FISA materials is a final order for purposes of appeal. See 50 U.S.C. § 1806(h). In the unlikely event that the Court orders disclosure of any item within any of the FISA materials, given the significant national security consequences that would result

B. THE LAW APPLICABLE TO FISA COLLECTION (U)

Each of the FISA applications and orders at issue in this case meet all of the statutory requirements to include probable cause and the fruits of the FISA collection should not be suppressed. As the Court's *in camera, ex parte* review of the FISA materials will show, the requisite probable cause standards were amply satisfied here for the FISC-authorized collection at issue; the applications contained the proper certifications; and such certifications were not clearly erroneous. Moreover, even if this Court disagrees with the FISC's repeated determinations in each of its orders, the evidence obtained from any FISA surveillance still should not be suppressed because the FBI acted in good faith in conducting the surveillance. (U)

(1) Statutory Requirements (U)

The FISC may only approve electronic surveillance if it finds, among other things, that:

> [O]n the basis of the facts submitted by the applicant there is probable cause to believe that —
>
> (A) the target of the electronic surveillance is a foreign power [14] or an agent of a foreign power: *Provided*, that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
>
> (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an

---

from such disclosure, the United States expects to pursue an appeal. Accordingly, the United States respectfully requests that the Court indicate its intent to do so before issuing an order, or that any such order be issued in a manner that the United States has sufficient notice to file an appeal prior to any actual disclosure. (U)

[14] "Foreign power" is defined in 50 U.S.C. § 1801(a). For purposes of this case, a "foreign power" includes a "group engaged in international terrorism or activities in preparation thereof." 50 U.S.C. § 1801 (a)(4). (U)

agent of a foreign power . . . .

50 U.S.C. § 1805(a)(3) (emphasis in original). "In determining whether or not probable cause exists for purposes of an order under subsection (a)(3), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." Id. at § 1805(b). (U)

As it relates to United States citizens or aliens lawfully admitted for permanent residence, "agent of a foreign power" means:

> [A]ny person who —
>
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power,[] which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism,[15] or

---

[15] "International terrorism" is defined as activities that —

> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
>
> (2) appear to be intended —
>
> > (A) to intimidate or coerce a civilian population;
> >
> > (B) to influence the policy of a government by intimidation or coercion; or
> >
> > (C) to affect the conduct of a government by assassination or kidnaping; and

> activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power;[16] or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Id. at § 1801(b)(2). (U)

With respect to non-United States persons, an "agent of a foreign power" additionally includes a person who:

> (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section [i.e. "a group engaged in international terrorism or activities in preparation therefor"]; [or]
>
> (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities.

Id. at § 1801(b)(1), (2). (U)

> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. 50 U.S.C. § 1801(c). (U)

[16] FISA was amended in 1999 to add this definition of "agent of foreign power." (U)

(2) Standard of Review (U)

Where the statutory application has been properly made and approved by the FISC, it carries a "strong presumption of veracity and regularity in a reviewing court." United States v. Pelton, 835 F.2d 1067, 1076 (4th Cir. 1987); Accord United States v. Duggan, 743 F.2d at 77 & n.6 ("representations and certifications submitted in support of an application for FISA surveillance should be presumed valid.") Thus, when reviewing FISA materials to determine whether probable cause supported the conclusion that the target was an agent of a foreign power, and that each of the facilities or places at which the FISA collection was directed, was being used or was about to be used by the target, a district court should act as it would if it were reviewing a probable cause determination made in connection with the issuance of a criminal search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure, or a criminal wiretap approved pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), codified at 18 U.S.C. §§ 2510 et seq. (U)

The probable cause standard in the criminal search warrant and Title III contexts is not a stringent one. As the Supreme Court has stated, the "task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983); see United States v. Brundidge, 170 F.3d 1350, 1352 (11th Cir. 1999.) Such determinations must be approached in a practical way, because probable cause is a "flexible, common-sense standard." Texas v. Brown, 460 U.S. 730, 742 (1983); Brundidge, 170 F.3d at 1352. Moreover, the "duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable

cause existed." Gates, 462 U.S. at 238 (internal quotes omitted); see also United States v. Miller, 24 F.3d 1357, 1363 (11th Cir. 1994) ("[R]eviewing courts lend substantial deference to an issuing magistrate's probable cause determinations.") (U)

In the FISA context, federal district court judges sitting on the FISC should receive as much deference as a magistrate or a district court judge in a criminal search warrant or Title III context. Thus, in accord with the case law discussed above, the government respectfully submits that this Court should give "substantial deference" to the FISC when examining the FISA materials, should resolve doubts "in favor of upholding the warrant," and should confine its review to a determination as to whether there was a "fair probability" that the target was an agent of a foreign power and that the object of the surveillance was used by or was about to be used by such an agent. Finally, and importantly, in the FISA context, the standard is not whether there was probable cause to believe that foreign intelligence information would, in fact, be found; rather, the standard is whether, applying the applicable law and standard of review, the FISC correctly concluded that there was probable cause to believe that the target was an agent of a foreign power, and that the facilities or places at which the electronic surveillance was directed, were being used or were about to be used by the foreign power or agent of the foreign power. See 50 U.S.C. § 1805 (a)(3); United States v. Duggan, 743 F.2d at 73; United States v. Belfield, 692 F.2d at 147 (a reviewing court should "determine whether the application and order comply with the statutory requirements.") (U)

After an *in camera, ex parte* review, the Court should uphold the FISC's orders and find that probable cause existed to believe that each target was an agent of a foreign power and that each target was using, or was about to use, the facilities at which the surveillance was directed.

(U)

(3) The First Amendment (U)

The Court's *in camera* and *ex parte* review of the FISA materials will also show that none of the FISC's probable cause findings regarding any of the United States person targets of FISA surveillance were based solely upon activities protected by the First Amendment. Any argument that the FISA evidence should be suppressed on this ground should therefore be rejected.[17] (See Hassoun Mot. to Suppress at 13.) (U)

Among the findings the FISC's required to make prior to authorizing foreign intelligence collection targeting a United States person is the finding that there is probable cause to believe that the target of the electronic surveillance is a "foreign power or an agent of a foreign power." See, e.g., 50 U.S.C. § 1805(a)(3). FISA specifically provides, however, that "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the Constitution of the United States." Id. (Emphasis supplied.) (U)

Just as the First Amendment does not protect the defendant from prosecution on the charges alleged in the superseding indictment, the First Amendment does not prohibit the FISC from making conclusions in regard to a target's activities. See Rahman, 861 F. Supp. at 252 (holding that statements that are arguably protected speech may constitute evidence that the defendant was an agent of a foreign power); Falvey, 540 F. Supp. at 1314 (affirming FISC order

---

[17] We note that FISA does not prohibit probable cause from being based solely on protected First Amendment activity with respect to targets who are not United States persons. See 50 U.S.C. § 1805(a)(3). As the Court's *in camera, ex parte* review will show, however, protected First Amendment activity did not form the sole basis of the FISC's finding of probable cause with respect to any target in this case. (U)

and rejecting argument that engaging in terrorist activities on behalf of Irish Republican Army is protected by the First Amendment, even though "the object of the IRA's activities is to unite the North and South of Ireland," because "it is equally manifest that the IRA engages in international terrorism.") (U)

For example, even though establishing a nonprofit organization can be lawful activity, it certainly can be considered as part of the basis of a probable cause determination when an organization is used to conduct, or further, the affairs of an international terrorist group. Indeed in Rahman, the targets' conversations or speeches were not "simply the expression of ideas," but rather, constituted permissible evidence that the targets were agents of a foreign power. See Rahman, 861 F. Supp. at 254. (U)

The FISA collection at issue in the instant case was authorized by the FISC after a careful review of the applications that were submitted to it by the government. With respect to each application, the FISC held that all of the requirements of the statute were met, and the FISC's probable cause determinations were not based solely upon activities that were protected by the First Amendment. Indeed, under the express terms of FISA, each judge of the FISC that considered each application in the instant case could not have approved the FISA collection unless it complied with the statute, including the First Amendment proviso. This Court's *in camera* and *ex parte* review of each of the applications and orders will confirm that each judge of the FISC correctly made those findings with respect to each FISA application at issue, and that the sole basis for the FISA collection was not activities protected by the First Amendment. (U)

(4) This Court Should Not Suppress The FISA Evidence Even If This Court Disagrees With The FISC's Findings Of Probable Cause (U)

Even assuming *arguendo* that this Court — contrary to the FISC — finds that a particular

FISC order was not supported by probable cause, the FISA evidence obtained pursuant to that order is, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in United States v. Leon, 468 U.S. 897 (1984). Although no court has yet addressed the application of Leon's good faith exception to a FISC order, precedent from the Title III context supports its application. (U)

In this regard, the district court's opinion in United States v. Ambrosio, 898 F. Supp. 177 (S.D.N.Y. 1995), is instructive. In Ambrosio, the district court analyzed conflicting precedent on the question of whether the good faith exception applied to wiretap warrants issued pursuant to Title III. See id. at 187 & n.11 (citing cases on both sides of issue.) Ultimately, the court held that the good faith exception applied to Title III wiretap warrants for two reasons. First, the court concluded that amendments to Title III and the statute's legislative history demonstrated a Congressional intent that Title III would be "applied consistently with constitutional requirements" such as Leon's good faith exception. See id. at 187-88; see also United States v. Moore, 41 F.3d 370, 376 (8th Cir. 1994) (noting that the "legislative history expresses a clear intent to adopt suppression principles developed in Fourth Amendment cases.") Second, the court held that Title III wiretap applications are subject to good faith analysis under Franks v. Delaware, 438 U.S. 154 (1978), and "Leon's good faith analysis is an integral part of a Franks analysis." See id. at 188-89. (U)

Like Title III, FISA contemplates its own application to be consistent with constitutional requirements. Subsection 1806(g) provides:

> If the United States district court pursuant to subsection (f) of this section [regarding *in camera* and *ex parte* review of suppression motions] determines that the surveillance was not lawfully authorized or conducted, it shall, ***in accordance with the***

> ***requirements of law***, suppress the evidence which was unlawfully obtained or derived . . . .

50 U.S.C. § 1806(g) (emphasis added.) Because subsection 1806(g) requires application generally of "the requirements of law," constitutional principles – such as Leon's good faith exception – should apply to FISA suppression motions.[18] Moreover, like Title III applications, one federal appellate court has stated that FISA applications are subject to good faith analysis under Franks. See Duggan, 743 F.2d at 77 n.6 (opining that Franks principles apply to review of FISA orders.) Thus, Leon's good faith exception should apply in the FISA context. (U)

The FISA surveillances at issue in this case squarely fall within the "good faith exception." Leon and its progeny outline four situations to which the Leon "good faith exception" does not apply: (1) when the Magistrate Judge issued the warrant in reliance on a deliberately or recklessly false affidavit; (2) when the Magistrate Judge failed to act in a neutral and detached manner; (3) when the warrant was based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) when the warrant was so facially deficient that a reasonable officer could not have believed it to be valid. See Leon, 468 U.S. at 914-15; see also Massachusetts v. Sheppard, 468 U.S. 981, 988 (1984).

---

[18] It should be noted that Title III, which was enacted in 1968, was amended in 1986, two years after Leon was decided. The 1986 Title III amendments "limit[ed] the statute's remedies and sanctions to nonconstitutional violations . . . so that in the event a violation of constitutional magnitude occurs, 'the court . . . will apply the existing Constitutional law with respect to the exclusionary rule.'" Ambrosio, 898 F. Supp at 187 (emphasis omitted) (quoting legislative history to Title III amendments.) FISA was enacted in 1978, six years before Leon was decided. The USA PATRIOT Act's amendments to FISA did not address this issue and its legislative history does not discuss it. Nonetheless, FISA's textual support for applying extra-statutory law such as Leon's exclusionary rule is more compelling than that in Title III. Compare 50 U.S.C. § 1806(g) ("in accordance with the requirements of law") with 18 U.S.C. § 2518(10) ("The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.") (U)

None of these situations are present here. (U)

As discussed *infra*, there is no basis to find that the declarations or certifications submitted in support of the FISA applications at issue in this case were deliberately or recklessly false. With respect to the second situation, the defendant does not present any facts indicating that the independent Article III judges on the FISC failed to act in a neutral and detached manner in repeatedly issuing the pertinent FISC orders. Regarding the third and fourth situations, as the Court will see in its *in camera, ex parte* review of the FISA materials and as is discussed herein, the documents submitted in support of the FISC's orders provided abundant facts that established the requisite probable cause and each of those orders contained all of the requisite findings. For these reasons, the FISA evidence obtained pursuant to that order should, nonetheless, be admissible under Leon's "good faith" exception to the exclusionary rule. (U)

(5) FISA's Certification Requirements As To The Purpose Of The Surveillances Were Satisfied (U)

Defendant Hassoun next argues that the FISA surveillance was illegal because the purpose of the surveillance was improper. (Hassoun Motion at 13-14.) Essentially defendant claims that the primary purpose of the surveillance was not to obtain foreign intelligence information, but rather was to obtain evidence for use in a criminal investigation. Hassoun, therefore, implies that the certification of the purpose of the surveillance in the FISA applications was clearly erroneous. In support of his assertion, the defendant speculates that the investigation was premised upon an investigation into the criminal activities of Sheikh Omar Abdel Rahman and his supporters, which he then suggests taints the purpose of any subsequent FISA surveillance. Virtually the same argument was rejected in the case against several individuals connected to Sheikh Omar Abdel Rahman, including his attorney Lynne Stewart. Sattar, 2003

WL 22137012 (S.D.N.Y.). (U)

The defendant's argument is flawed because it is based on the erroneous premise that FISA does not permit the United States to concurrently engage in a foreign intelligence investigation and a criminal investigation. Moreover, the fact that information obtained through FISC-authorized surveillance may be shared between intelligence and law enforcement agents does not affect the government's certification of the purpose of the surveillance. This Court's *in camera* and *ex parte* review of the FISA materials will demonstrate that the certifications regarding the purpose of the surveillance were not clearly erroneous. Under any standard, either before or after the USA PATRIOT Act, the FISA collection was clearly lawful and as such should be upheld.[19] (U)

(a) Standard of Review of Certification Requirement (U)

The certifications submitted in support of FISA applications should be "presumed valid." Duggan, 743 F.2d at 77 n.6. For this reason, it is well established that FISA certifications are to be "subjected to only minimal scrutiny by the courts." Badia, 827 F.2d at 1463; see also In re: Grand Jury Proceedings of the Special April 2002 Grand Jury, 347 F.3d at 205; Duggan, 743

---

[19] It is beyond dispute that fruits of valid FISA surveillance are properly used in a criminal trial, under either the pre- or post-USA PATRIOT Act standard of review. Indeed, section 1806 expressly contemplates such use. See 50 U.S.C. § 1806(b). Moreover, throughout FISA's history, courts - including the Eleventh Circuit - have uniformly so stated. See Badia, 827 F.2d at 1464 (pointing out that "an otherwise valid FISA surveillance is not tainted simply because the government may later use the information obtained as evidence in a criminal trial. Indeed, FISA contemplates such use.") (internal citation omitted); see also In re Sealed Case, 310 F.3d at 727 ("In sum, we think that the FISA as passed by Congress in 1978 clearly did not preclude or limit the government's use or proposed use of foreign intelligence information [gathered under a FISC order] . . . in a criminal prosecution."); Duggan, 743 F.2d at 78 ("We emphasize that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by § 1806(b), as evidence in a criminal trial."); accord Johnson, 952 F.2d at 572; Pelton, 835 F.2d at 1075; Rahman, 861 F. Supp. at 251. (U)

F.2d at 77 (stating that a reviewing court should not "second-guess the executive branch official's certifications); Rahman, 861 F. Supp. at 249. In essence, "the reviewing court [is] to have no greater authority to review the executive branch's certifications than has the FISA judge." Badia, 827 F.2d at 1463; see also In re Grand Jury Proceedings, 347 F.3d at 204-5 (conducting same review.) (U)

Section 1805, which outlines the requisite findings necessary to issue a FISA order, requires that the FISC find that:

> the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the . . . certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

50 U.S.C. § 1805(a)(5). Following this standard, one district court explained its review of the FISC orders before it as follows:

> once a reviewing court – be it the [FISC] or this court – finds that an authorized executive branch official has certified [the purpose], and his certification is supported by probable cause to believe that the target is an agent of a foreign power as defined in the statute, and that the location is one being or to be used by the target, and it appears from the application as a whole that that certification is not clearly erroneous, the task of that court is at an end.

Rahman, 861 F. Supp. at 251 (citations omitted.) Likewise, courts collaterally reviewing the

purpose of FISA surveillance have uniformly applied the "clearly erroneous" standard.[20] See, e.g., Hammoud, 381 F.3d at 333; Sattar, 2003 WL 22137012, at *13; also Badia, 827 F.2d at 1463; Duggan, 743 F.2d at 77. (U)

In 2001, Congress enacted the USA PATRIOT Act and abolished what some courts had described as FISA's "primary purpose" test. Sattar, 2003 WL 22137012 at *11. The Foreign Intelligence Surveillance Court of Review ("FISC of Review") articulated the standard of review of post-USA PATRIOT Act FISA applications as similarly deferential:

> [W]e think the government's purpose as set forth in a section 1804(a)(7)(B) certification is to be judged by the national security official's articulation and not by a [FISC] inquiry into the origins of an investigation nor an examination of the personnel involved. It is up to the Director of the FBI, who typically certifies, to determine the government's national security purpose, as approved by the Attorney General or the Deputy Attorney General. . . . The important point is that the relevant purpose is that of those senior officials in the Executive Branch who have the responsibility of appraising the government's national security needs. Id. at 736. (U)

Under these legal principles, therefore, this Court should apply the same standard as the FISC when reviewing the certifications contained in the challenged FISA applications. First, the Court should verify that the certifications state that the "purpose," or a "significant purpose," of the surveillance was to collect foreign intelligence information based on whether the collection

---

[20] Indeed, there is a strong argument that there should be no judicial review of the purpose of pre-USA PATRIOT Act FISA surveillance based on FISA's text. Sections 1805(a)(1) to (a)(5) require the FISC to make certain findings before issuing an order approving FISA surveillance. None of these findings includes an analysis of the purpose of the surveillance. If the FISC (pre-USA PATRIOT Act) was not empowered to review the purpose of a particular surveillance application, then, *a fortiori*, a court reviewing the FISC's order (issued pre-USA PATRIOT Act) is not empowered to review whether the FISC's evaluation of purpose was in error. Instead, the district court's review should be limited to a determination of whether the application and the FISC order **contains** the appropriate certifications. See In re Sealed Case, 310 F.3d at 723-24. At the very least, this strongly supports the argument made herein that the district court's purpose review is highly deferential. (U)

was either pre-USA PATRIOT Act or subsequent to that Act. If the target was not a United States person, the Court's inquiry should end. If the target was a United States person, the Court should then determine whether the certifications were clearly erroneous based on the statements regarding the basis for the certification and any other additional information in the applications. 50 U.S.C. § 1805(a)(5). A finding is "clearly erroneous" when, although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed. See United States v. U.S. Gypsum Co., 333 U.S. 364, 395 (1948); United States v. White, 335 F.3d 1314, 1319 (11th Cir. 2003). (U)

(b) Neither Concurrent Criminal and Foreign Intelligence Investigations Nor Information-Sharing Between Intelligence and Law Enforcement Agents Negates the Government's Certification of Purpose (U)

Hassoun essentially asserts that the FISA surveillance at issue was conducted primarily for the purpose of obtaining criminal evidence because a criminal investigation of Sheik Rahman and his supporters was also being conducted. His contention is based on a fundamental misunderstanding of the FISA statute and the relevant case law. (U)

First, nothing in FISA prohibits the government from engaging in a criminal and a foreign intelligence investigation. To the contrary, it is common for criminal and foreign intelligence investigations to occur concurrently. Indeed, the definition of "agent of a foreign power" includes persons who engage in certain activities that "involve or may involve" violations of federal criminal law. See 50 U.S.C. § 1801(b)(2); see also In re Sealed Case, 310 F.3d at 723. (U)

Moreover, the government's "foreign policy concerns [do not] recede" simply because it begins to move towards criminal prosecution of a target. See In re Sealed Case, 310 F. 2d at 743.

As the FISC of Review noted, in the counterintelligence field, criminal prosecutions "can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts." Id. Thus, the relevant inquiry is not the nature of the underlying investigation, but rather the general purpose of the surveillance. See id. at 728. As the Court's *in camera* and *ex parte* examination of the certifications accompanying the FISA applications will show, the electronic surveillance authority was obtained in order to collect foreign intelligence information. Because there is nothing inherently improper about overlapping criminal and foreign intelligence investigations, Hassoun's request for disclosure of such information should be denied. (U)

Second, nothing in FISA prohibits sharing FISA-derived information with criminal investigators under the proper circumstances and in compliance with certain procedures. Indeed, it is well established that FISA permits the sharing of FISA information with criminal prosecutors, as well as consultations between intelligence and criminal investigators regarding FISA surveillance. See In re Sealed Case, 310 F.3d at 728 (noting that the intelligence sharing procedures effective after 1995 permitted "significant information sharing and coordination" between criminal and foreign intelligence investigations.) Thus, a claim that dissemination of FISA information to criminal investigators violates FISA is meritless. (U)

To further clarify, the often referenced "wall," was not an impermeable barrier surrounding FISA-obtained or derived information to prevent it from being shared with criminal investigators or prosecutors. Rather, the "wall" was a reference to the way certain Department of Justice personnel narrowly interpreted the Department's intelligence sharing procedures to avoid "running afoul" of the primary purpose test, which was itself rejected by the FISC of Review. See In re Sealed Case, 310 F.2d at 727-28. Under the Department's internal procedures, FBI

criminal investigators and government prosecutors were not permitted to review all of the raw FISA intercepts or seized materials immediately upon their interception. See id. Instead, a screening person, who was not involved in the criminal investigation, would review the FISA intercepts and disseminate information that might constitute evidence relevant to a criminal investigation. See id. Thus, the mere fact that FISA-obtained or derived information may have been transmitted to criminal prosecutors or investigators does not support a conclusion that the self-imposed, narrowly-interpreted and so-called "wall" was improperly breached, let alone that the intelligence investigations were conducted for an improper criminal purpose. (U)

As the Court's *in camera* and *ex parte* review of the FISA materials will show, the certifications here tracked and satisfied section 1804 (a)(7)(B)'s requirement that a high-ranking Executive Branch officer certify that the purpose (for pre-USA PATRIOT Act application,) or a significant purpose (for applications filed after passage of the USA PATRIOT Act) of the surveillance was to obtain foreign intelligence information. Furthermore, none of the certifications were clearly erroneous. (U)

(6) FISA's Requirement That The Information Could Not Reasonably Be Obtained By Normal Investigative Techniques Was Satisfied (U)

The Court should review this portion of the certification under the same standard of review that applied to its review of the purpose certification and find that the certifications were not clearly erroneous. (U)

FISA requires that a high-ranking Executive Branch official certify in each application that the foreign intelligence information sought "cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1804(a)(7)(C). When issuing an order, the FISC must find that the application contains all of the certifications required by section 1804 and, if the

target is a United States person, that the certifications are not clearly erroneous. 50 U.S.C. § 1805(a)(3). Just as with the certification of the purpose of the surveillance, the FISC's determination here should be given substantial deference by the reviewing court. See, e.g., Badia, 827 F.2d at 1463 (FISA certifications are to be "subjected to only minimal scrutiny by the courts.") Accordingly, the reviewing court should employ the same standard of review as the FISC. See id. at 1463. (U)

With respect to United States person targets, "clearly erroneous" is the appropriate standard of review. See 50 U.S.C. § 1805(a)(5). With respect to non-United States person targets, the Court should simply review the pertinent applications to verify that they "contain[] all statements required by section 1804." See 50 U.S.C. § 1805(a)(5). (U)

The Court's *in camera* and *ex parte* review of each of the FISA applications will show that they contained the requisite certification regarding the necessity for the surveillance, and all of the requisite statements under § 1804. Accordingly, this Court should reach the same conclusion as the FISC, that the certifications were not clearly erroneous. (U)

(7) Hassoun Has Failed To Establish the Requisite Preliminary Showing Necessary to Obtain a Hearing Pursuant to Franks v. Delaware, 438 U.S. 154 (1978) (U)

Hassoun argues that the Court should suppress the FISA evidence if it contains intentionally false statements or material omissions. For the most part, Hassoun bases his request on pure speculation, referencing nothing more than the errors cited by the FISC in seventy-five unrelated applications. See Hassoun Mot. to Suppress at 2, 14-16. The defendant's generalized and unsupported allegations of potential misstatements and omission is woefully deficient and does not come close to satisfying the Franks standard. (U)

Affidavits supporting search warrants are presumed valid. Franks v. Delaware, 438 U.S. 154, 171 (1978). In Franks, the Supreme Court recognized the limited constitutional right of a criminal defendant to attack the veracity of a warrant affidavit. United States v. Cross, 928 F.2d 1030, 1040 (11th Cir. 1991). The United States was unable to find any cases expressly holding that the rule of law announced in Franks applies to FISA applications and orders. However, at least one court of appeals has noted, in dicta, that if there were an allegation that the United States obtained a FISA order based on fraudulent representations, review of that argument should be governed by the principles set forth in Franks v. Delaware. See Duggan, 743 F.2d at 77 n.6; see also 50 U.S.C. § 1806(g) (suppression remedy is to be "applied in accordance with the requirements of law.") (U)

To merit an evidentiary hearing under Franks, the defendant must first make a "concrete and substantial preliminary showing" that: (1) the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit; and (2) the misrepresentation was essential to the finding of probable cause. Franks, 438 at 155-56; Cross, 928 F.2d at 1040. The district court must require the defendant to meet both of these elements prior to conducting an evidentiary hearing. West Point-Pepperell v. Donovan, 689 F.2d 950, 959 (11th Cir. 1982). (U)

The defendant's "attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." Franks, 438 U.S. at 171. Rather, the defendant must submit allegations of deliberate falsehood or of reckless disregard for the truth accompanied by an offer of proof. Id. Allegations of negligence or innocent mistake are insufficient, id., as are allegations of insignificant or immaterial misrepresentations or omissions. United States v.

Jenkins, 901 F.2d 1075, 1080 (11th Cir. 1990.) Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing still should not be held if the affidavit provides probable cause when the allegedly false material is eliminated or the omitted information is included. Id. at 171-72; see also United States v. Sims, 845 F.2d 1564, 1571 (11th Cir. 1988). (U)

As explained *supra*, there is nothing unique about this case that would require disclosure of the FISA materials or an evidentiary hearing, and the defendant has failed to make the required Franks showing. If a defendant could force disclosure of FISA materials and obtain an adversarial hearing merely by speculating that there might be a Franks violation, then disclosure of FISA materials and adversarial hearings would be the rule and not the exception. Such a result would violate Congress' clear intent that FISA materials should be reviewed *in camera* and *ex parte* and in a manner that is consistent with the realities of modern intelligence gathering needs and investigative techniques. In keeping with the well-established principle in the search warrant context that a defendant may only obtain a Franks evidentiary hearing after making a "concrete and substantial preliminary showing," Hassoun should at least be required to make such a showing before disclosure of any FISA materials or an adversarial hearing on Franks grounds can even be seriously considered. (U)

Hassoun's argument that he is unable to make such a preliminary showing because he does not have access to the affidavits does not advance his cause. Such will always be the quandary for defense counsel in cases involving FISC-authorized surveillance. Yet, as Congress and the courts have recognized, that difficulty does not justify disclosure of FISA materials:

> We appreciate the difficulties of appellant's counsel in this case. They must argue that the determination of legality is so complex that an

> adversary hearing with full access to relevant materials is necessary. But without access to the relevant materials their claim of complexity can be given no concreteness. It is pure assertion.
> Congress was also aware of these difficulties. But it chose to resolve them through means other than mandatory disclosure. In FISA Congress has made a thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence. . . . Appellants are understandably reluctant to be excluded from the process whereby the legality of a surveillance by which they were incidentally affected is judged. But it cannot be said that this exclusion rises to the level of a constitutional violation.

Belfield, 692 F.2d at 148.[21] (U)

In short, at this point, Hassoun's attack under Franks is largely non-specific and unsupported. In contrast, the Declaration of a high ranking FBI official informs this Court, in concrete detail, all of the reasons that disclosure of the FISA materials would endanger national security. Balancing the United States' specifically-supported need to protect national security against Hassoun's speculative desire to examine the FISA materials and taking into account the Congressionally-mandated presumption of non-disclosure for FISA materials, the applicable case law under FISA and Franks and its progeny, this Court must deny the defendant's request for disclosure of the FISA materials and an adversary hearing under Franks.[22] (U)

(8) Minimization Under FISA (U)

FISA contains a requirement that the Attorney General establish minimization procedures

---

[21] Indeed, it should be noted that even in the context of a review of electronic surveillance conducted pursuant to Title III, the Supreme Court has held that adversary proceedings are not always constitutionally required. Giordano v. U.S., 394 U.S. 310, 314 (1969); Taglianetti v. U.S., 394 U.S. 316, 317 (1969). (U)

[22] Pursuant to FISA, e.g., 50 U.S.C. § 1806(f), however, the United States has requested that the Court determine that the FISC-authorized collection was lawfully authorized and conducted on the basis of an *in camera, ex parte* review of the FISA materials. Should any defendant later seek to raise any additional arguments regarding the conduct of the FISC-authorized collection, the United States reserves the right to submit further briefing. (U)

that regulate the acquisition, retention and dissemination of information about United States persons which is obtained through FISA collection, including persons who are not the targets of the FISA collection. FISA requires that minimization procedures be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. § 1801(h)(1). In addition, "notwithstanding" the definition set forth above, minimization procedures also mean "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. § 1801(h)(3). (U)

FISA's definition of "[f]oreign intelligence information" includes information that "relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power [and/or] sabotage or international terrorism by a foreign power or an agent of a foreign power." 50 U.S.C. § 1801(e). "Foreign intelligence information" also includes information with respect to a "foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e)(2). (U)

In order to fulfill the statutory requirements discussed above, the Attorney General has approved standard minimization procedures for FISA collection. These standard minimization

procedures are on file with the FISC, and are incorporated by reference into every FISA application that is submitted to the FISC. As a result, in connection with the investigation that led to the indictment in the above-captioned case, every FISA judge that issued an order authorizing the FISA collection found that the standard applicable minimization procedures that were incorporated by reference, as well as any additional minimization procedures that may have been proposed, met the statutory requirements. Thereafter, each FISA order directed that the approved minimization procedures be followed in conducting the FISA collection. (U)

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence. For example, the activities of individuals engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. See United States v. Rahman, 861 F. Supp. at 253 (rejecting the notion that the "wheat" could be separated from the "chaff" while the "stalks were still growing.") Indeed, foreign powers and their agents frequently use ambiguous, guarded or coded language as well as false identities and compartmentalized functions and other practices to conceal their full organization, activities and plans. See In re Sealed Case, 310 F.3d at 741; see also United States v. Salameh, 152 F.3d 88, 154 (2d Cir. 1998) (noting that the bombing conspiracy was discussed in code.) (U)

As a result, "[l]ess minimization in the acquisition stage may well be justified" when the "'investigation is focusing on what is thought to be a widespread conspiracy [where] more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise.'" In re Sealed Case, 310 F.3d at 741 (citing Scott v. United States, 436 U.S. 128, 140

1978) (acquisition of virtually all conversations was reasonable under the circumstances); accord United States v. Bin Laden, 126 F. Supp. 2d at 286 ("more extensive monitoring and 'greater leeway' in minimization efforts" is permitted in certain investigations.) Accordingly, FISA surveillance devices are normally left on continuously and the government is "not required to make an instantaneous identification of information acquired through a FISA authorized surveillance as unequivocally being foreign intelligence or else discarding it." In re Sealed Case, 310 F.3d at 741; United States v. Thomson, 752 F. Supp. at 81 (it is permissible to retain and disseminate "bits and pieces" of information until their "full significance becomes apparent"); House Report at 58 (same.) (U)

The federal courts therefore afford the government "flexibility" in trying to discern the meaning of communications between agents of foreign powers because "[i]nnocuous-sounding conversations" may later prove to be "signals of important activity," and because "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." In The Matter of Kevork, 634 F. Supp. 1002, 1017 (C.D. Ca. 1985), aff'd on other grnds, 788 F.2d 566 (9th Cir. 1986); United States v. Rahman, 861 F.Supp. at 252-53. Indeed, as one court has stated, when a United States person communicates with an agent of a foreign power, the government "would be remiss in meeting its foreign counterintelligence responsibilities if it did not investigate such contacts and gather information to determine the nature of those activities." United States v. Thomson, 752 F.Supp. at 82. (U)

The legislative history of FISA further illustrates this point. When a United States person is involved in clandestine intelligence activities, it is "necessary" to retain his or her

communications in order to identify other individuals who may be involved, even if those communications relate to "innocent persons." The need to retain and conduct a thorough post-acquisition review of FISA information exists:

> where the Government is wiretapping a known spy, who is a U.S. person. It is "necessary" to identify anyone working with him in his network, feeding him his information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report at 58. (U)

As Congress further recognized, however, the "failure to gather further incriminating information concerning the contacts or acquaintances of the spy does not necessarily mean they are in fact innocent – instead, they may merely be very sophisticated and well-versed in their espionage tradecraft." Id. Accordingly, in order to pursue "leads," Congress intended that the government be given "a significant degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." Id. Minimization practices of the government should not, therefore, be examined with hindsight. Rather, as the Supreme Court has stated, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." Scott v. United States, 436 U.S. at 136; id. at 140-142. (U)

Minimization takes place at the acquisition, retention and/or the dissemination stage of an investigation in regard to FISA communications. As a result, as the Senate Select Committee on Intelligence observed in its final report, in certain situations, "primarily for technological reasons,

it may not be possible to avoid acquiring all conversations. In these situations, minimizing at the retention and dissemination stages becomes most important." Senate Intelligence Report at 40; See also In The Matter of Kevork, 634 F. Supp. at 1017 ("minimization may occur at any of several stages.") (U)

In light of the realities associated with the collection of foreign intelligence information pursuant to FISA, Congress recognized that minimization efforts by the government can never be mistake-free since "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." Senate Intelligence Report at 40. The Fourth Circuit reached the same conclusion in United States v. Hammoud, 381 F.3d at 334 ("mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance.") As the Fourth Circuit stated:

> it is not always immediately clear into which category a particular conversation falls. A conversation that seems innocuous on one day may later turn out to be of great significance, particularly if the individuals involved are talking in code.

Id. (citation omitted); see also United States v. Ott, 637 F. Supp. at 64; United States v. Thomson, 752 F. Supp. at 80. (U)

Thus, in reviewing the adequacy of minimization efforts in complex investigations over long periods of time, the government is permitted to minimize communications consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence based on circumstances then known by the agents, 50 U.S.C. § 1801(h)(1), and the test to be applied by the federal courts is not whether innocent communications were intercepted or whether mistakes were made with respect to certain communications. Rather:the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have

done all they reasonably could to avoid unnecessary intrusion." Absent a charge that the minimization procedures have been completely disregarded, the test of compliance is "whether a good faith effort to minimize was attempted. Senate Intelligence Report at 39-40; Accord United States v. Hammoud, 381 F.3d at 334 (government must make a "good faith" effort to minimize); see also United States v. Ruhe, 191 F.3d 376, 383 (4th Cir. 1999) ("properly seized evidence may be excluded when the officer's executing the warrant exhibit a flagrant disregard for its terms.") (U)

Moreover, FISA expressly states that the government is not required to minimize information that is "evidence of a crime." 50 U.S.C. § 1801(h)(3). As a result, to the extent that certain communications of a United States person establish an element of a substantive or conspiratorial offense, such communications need not be minimized. See United States v. Isa, 923 F.2d 1300, 1305 (8th Cir. 1991). The government, however, is not required to terminate surveillance and make an arrest when evidence of a crime is uncovered. In an intelligence investigation, as the Congress pointed out, it may be "more fruitful" to "monitor" the activities of terrorists in the United States to "identify otherwise unknown terrorists here, their international support structure, and the location of their weapons or explosives." House Report at 43-44; see United States v. United States District Court (Keith), 407 U.S. 297, 322 (1972) (national security surveillance is "often long range and involves the interrelation of various sources and types of information"); See Senate Intelligence Report at 11 ("Surveillances conducted under [FISA] need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate.") (U)

Similarly, "prosecutors are under no duty to file charges as soon as probable cause exists

but before they are satisfied they will be able to establish the suspect's guilt beyond a reasonable doubt." United States v. Lovasco, 431 U.S. 783, 791 (1977). Thus, even with respect to FISA collections that continue for years, the length of the collection in any particular case does not undermine the repeated findings of the FISC that all of the requirements of the statute have been met and that the surveillance may lawfully continue. See Sattar, 2003 WL 22137012, at *2, 6, 8 (2003) (where the court reviewed "voluminous" FISA materials concerning FISC-authorized surveillance that continued for a "period of several years.") (U)

Finally, even assuming *arguendo,* that certain communications were not properly minimized in any given case, suppression is not the appropriate remedy with respect to the communications that were properly obtained and retained. As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that a court might conclude that some communications should have been minimized does not affect the admissibility of items properly seized. Indeed, Congress specifically intended that the only evidence that should be suppressed is the "evidence which was obtained unlawfully":

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

House Report at 93.

In camera and *ex parte* review of the FISA materials will show that the FISC-authorized collection at issue satisfied FISA's minimization requirements and the collection was lawfully conducted. (U)

C. THE FISA COLLECTION AT ISSUE (U)

Hassoun argues that the FISA-obtained evidence should be suppressed if it is established that there was no probable cause to believe that he or any other party under surveillance were agents of a foreign power. (See Hassoun Mot. to Suppress at 10-13; Hassoun Mot. To Produce at 1-2.) (U)

As the Court's *in camera* and *ex parte* review of the FISA materials will show, the FISC in each instance properly found probable cause to believe that each target was an agent of a foreign power and that each target was using, or was about to use, the facilities at which any surveillance was directed. In addition, the Court will see that the FISC's repeated findings of probable cause complied with all statutory requirements to include that probable cause for surveillance of any United States' person was not based solely on First Amendment-protected activities. Thus, Hassoun's claims should be rejected. (U)

[CLASSIFIED INFORMATION REDACTED]

(1) [CLASSIFIED INFORMATION REDACTED]

(a) [CLASSIFIED INFORMATION REDACTED]

(b) [CLASSIFIED INFORMATION REDACTED]

(2) [CLASSIFIED INFORMATION REDACTED]

(a) [CLASSIFIED INFORMATION REDACTED]

(b) [CLASSIFIED INFORMATION REDACTED]

(c) [CLASSIFIED INFORMATION REDACTED]

(3) [CLASSIFIED INFORMATION REDACTED]

(a) [CLASSIFIED INFORMATION REDACTED]

(b) [CLASSIFIED INFORMATION REDACTED]

(c) [CLASSIFIED INFORMATION REDACTED]

(d) [CLASSIFIED INFORMATION REDACTED]

(e) [CLASSIFIED INFORMATION REDACTED]

(f) [CLASSIFIED INFORMATION REDACTED]

(g) [CLASSIFIED INFORMATION REDACTED]

(h) [CLASSIFIED INFORMATION REDACTED]

(i) [CLASSIFIED INFORMATION REDACTED]

(4) [CLASSIFIED INFORMATION REDACTED]

(a) [CLASSIFIED INFORMATION REDACTED]

(b) [CLASSIFIED INFORMATION REDACTED]

(c) [CLASSIFIED INFORMATION REDACTED]

(d) [CLASSIFIED INFORMATION REDACTED]

(e) [CLASSIFIED INFORMATION REDACTED]

(f) [CLASSIFIED INFORMATION REDACTED]

(g) [CLASSIFIED INFORMATION REDACTED]

(h) [CLASSIFIED INFORMATION REDACTED]

(5) [CLASSIFIED INFORMATION REDACTED]

(a) [CLASSIFIED INFORMATION REDACTED]

(b) [CLASSIFIED INFORMATION REDACTED]

(c) [CLASSIFIED INFORMATION REDACTED]

(6) [CLASSIFIED INFORMATION REDACTED]

V. CONCLUSION (U)

Based upon the foregoing, this Court should conduct an *in camera* and *ex parte* review of all of the pleadings and materials submitted and find that the FISA-authorized collection at issue was lawfully authorized and lawfully conducted, the disclosure of FISA materials is not necessary, and the classified FISA materials should be maintained under seal. Accordingly, this Court should deny the defendant's motions in their entirety.

Respectfully submitted,

R. ALEXANDER ACOSTA
UNITED STATES ATTORNEY

Julia A. Paylor
Assistant United States Attorney
Fla. Bar No. 0724785
500 S. Australian Ave., Suite 400
West Palm Beach, Florida
Tel: (561) 820-8711
Fax: (561) 802-1787

Mark A. Maldonado
Trial Attorney
U.S. Department of Justice
Counterterrorism Section
950 Pennsylvania Ave., NW
Washington, D.C. 20530
Tel: (202) 353-3121
Fax: (202) 353-0778

CERTIFICATE OF SERVICE

I hereby certify that a true and exact copy of the foregoing has been sent via first-class United States Mail, postage prepaid, on this 5th day of April, 2006, to Kenneth M. Swartz, Counsel for Hassoun, 100 N. Biscayne Blvd., 21st Floor, Miami, Florida 33132; William W. Swor, Counsel for Jayyousi, 3060 Penobscot Building, 645 Griswold Street, Detroit, Michigan 48226; and Jeanne Baker, Co-Counsel for Hassoun, 2937 S.W. 27th Avenue, Suite 202, Miami, Florida 33133-3703.

R. ALEXANDER ACOSTA
UNITED STATES ATTORNEY

Julia A. Paylor
Fla. Bar No. 0724785
Assistant United States Attorney
500 S. Australian Ave., Suite 400
West Palm Beach, Florida 33401
Tel: (561) 209-1005
Fax: (561) 802-1787